**3GPP TSG-SA WG6 Meeting #37e S6-200652**

**E-meeting, 14th March – 26th May 2020 (revision of S6-200557)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.379** | **CR** | **0256** | **rev** | **2** | **Current version:** | **17.2.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Media plane security when using a functional alias as target address for private MCPTT calls | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Kontron Transportation | | | | | | | | | |
| ***Source to TSG:*** | S6 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eMONASTERY2 | | | | |  | ***Date:*** | | | 2020-05-11 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In order to support end-to-end media plane security between two MCPTT clients, it is required that the requesting client uses the MCPTT ID of the called party as a key to protect the media. If a functional alias as target address is used the same security algorithm shall be suppoted, which requires to change the current private call setup procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The private call procedure is modified to allow the requesting client to use a functional alias as target address and to protect the media by help of the MCPTT ID of the called party. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | End-to-end media security is not supported when functional alias is used as called party address. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 10.7.2.1.8 (new), 10.7.2.2.1, 10.7.2.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

##### 10.7.2.1.8 MCPTT functional alias resolution response

Table 10.7.2.1.8-1 describes the information flow MCPTT functional alias resolution response from the MCPTT server to the MCPTT client.

Table 10.7.2.1.8-1: MCPTT functional alias resolution response information elements

|  |  |  |
| --- | --- | --- |
| Information Element | Status | Description |
| MCPTT ID | M | The MCPTT ID of the calling party |
| MCPTT ID | M | The corresponding MCPTT ID of the called functional alias |

\* \* \* Next Change \* \* \* \*

##### 10.7.2.2.1 Private call setup in automatic commencement mode

The procedure focuses on the case where an MCPTT user is initiating an MCPTT private call for communicating with another MCPTT user, with or without floor control enabled, in an automatic commencement mode.

Procedures in figure 10.7.2.2.1-1 are the basic signalling control plane procedures for the MCPTT client initiating establishment of MCPTT private call with the chosen MCPTT user.

Pre-conditions:

1. The calling MCPTT user has selected automatic commencement mode for the call; or

2. The called MCPTT client is set to automatic commencement mode.

3. Optionally, MCPTT client 1 may use an activated functional alias for the call.

4. The MCPTT server has subscribed to the MCPTT functional alias controlling server within the MC system for functional alias activation/de-activation updates.



Figure 10.7.2.2.1-1: Private call setup in automatic commencement mode– MCPTT users in the same MCPTT system

1. MCPTT users on MCPTT client 1 and MCPTT client 2 are already registered for receiving MCPTT service, as per procedure in subclause 10.2.

2. User at MCPTT client 1 would like to initiate an MCPTT private call for the chosen MCPTT user. The MCPTT user at MCPTT client 1 may include a functional alias used within the MCPTT private call. For a private call with floor control, floor control is to be established.

3. MCPTT client 1 sends an MCPTT private call request towards the MCPTT server (via SIP core) using a service identifier as defined in 3GPP TS 23.228 [5] for MCPTT, for establishing a private call with the chosen MCPTT user. The MCPTT private call request contains the MCPTT ID or the functional alias of the invited user, an SDP offer containing one or more media types. For a private call with floor control, the MCPTT private call request also contains an element that indicates that MCPTT client 1 is requesting the floor. The MCPTT client 1 may include a Requested commencement mode that indicates that the call is to be established in automatic commencement mode if automatic commencement mode is requested by the initiating user.

NOTE 1: As part of this step, MCPTT client 1 and MCPTT client 2 set up a security association (when no functional alias is present), if end-to-end encryption is used for this call.

4. If the MCPTT private call request contains a functional alias instead of an MCPTT ID as called party and if end-to-end encryption shall be applied for this call, the MCPTT server shall resolve the functional alias to the corresponding MCPTT ID(s) for which the functional alias is active and proceed with step 5. Otherwise the MCPTT server checks whether the MCPTT user at MCPTT client 1 is authorized to initiate the private call, and that MCPTT user at MCPTT client 2 is authorized to receive the private call. If the MCPTT private call request requested automatic commencement mode then the MCPTT server also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a private call in automatic commencement mode and proceed with step 6.

5a. The MCPTT server shall resolve the functional alias to the corresponding MCPTT ID(s) for which the functional alias is active and responds with a functional alias resolution response message that contains the resolved MCPTT ID back to MCPTT client 1.

NOTE 2: If the MCPTT server detects that the functional alias used as the target of the private call request is simultaneously active for multiple MCPTT users, then the MCPTT server can proceed by selecting an appropriate MCPTT ID based on some selection criteria. The selection of an appropriate MCPTT ID is left to implementation. This selection criteria can include rejection of the call, if no suitable MCPTT ID is selected.

5b. If the MCPTT server replies with a MCPTT functional alias resolution response message, the MCPTT client 1 sends a new MCPTT private call request towards the resolved MCPTT ID.

NOTE 3: MCPTT client 1 and MCPTT client 2 set up a security association for the media, if end-to-end encryption is used for this call.

6. MCPTT server may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE 4: Step 6 can occur at any time following step 5b, and prior to step 10.

7. If authorized, MCPTT server includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request, includes the requested automatic commencement mode indication based on a requested automatic commencement mode by the calling user or based upon the setting of the called MCPTT client and sends the corresponding MCPTT private call request towards the MCPTT client 2, including the MCPTT ID and, if available, the functional alias of the calling MCPTT user 1. If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

8. The receiving MCPTT client 2 notifies the user about the incoming private call and displays the functional alias of calling MCPTT user 1.

9. The receiving MCPTT client 2 accepts the private call automatically, and an MCPTT private call response is sent to the MCPTT server (via SIP core).

10. Upon receiving the MCPTT private call response from MCPTT client 2 accepting the private call request, the MCPTT server informs the MCPTT client 1 about successful call establishment.

11. MCPTT client 1 and MCPTT client 2 have successfully established media plane for communication and either user can transmit media. For successful call establishment for private call with floor control request from MCPTT client 1, floor participant at MCPTT client 1 is granted floor by the floor control server, giving it permission to transmit. At the same time floor participant at MCPTT client 2 is informed by the floor control server that floor is taken.

\* \* \* Next Change \* \* \* \*

###### 10.7.2.2.2.2 Procedure

Both clients are served by the primary MCPTT service provider in figure 10.7.2.2.2.2-1.

Pre-conditions:

1. The calling MCPTT user has selected manual commencement mode or has not specified a commencement mode for the call; and

2. The called MCPTT client is set to manual commencement mode.

3. Optionally, MCPTT client 1 may use an activated functional alias for the call.

4. The MCPTT server has subscribed to the MCPTT functional alias controlling server within the MC system for functional alias activation/de-activation updates.



Figure 10.7.2.2.2.2-1: MCPTT private call in manual commencement mode– MCPTT users in the same MCPTT system

1. MCPTT client 1 and MCPTT client 2 are both registered and their respective users, MCPTT user 1 and MCPTT user 2, are authenticated and authorized to use the MCPTT service, as per procedure in subclause 10.2.

2. MCPTT user at MCPTT client 1 would like to initiate an MCPTT private call for the selected MCPTT user. The MCPTT user at MCPTT client 1 may include a functional alias used within the MCPTT private call. For a private call with floor control, floor control is to be established. For private call without floor control, both users will have the ability to transmit without floor arbitration.

3. MCPTT client 1 sends an MCPTT private call request addressed to the MCPTT ID of MCPTT user 2 using an MCPTT service identifier as defined in 3GPP TS 23.228 [5] (possible for the SIP core to route the request to the MCPTT server). The MCPTT private call request contains the MCPTT ID or the functional alias of invited user and an SDP offer containing one or more media types. The MCPTT private call request may also contain a data element that indicates that MCPTT client 1 is requesting the floor, for a private call with floor control. The MCPTT client 1 may include a requested commencement mode that indicates that the call is to be established in manual commencement mode if manual commencement mode is requested by the initiating user.

NOTE 1: As part of this step, MCPTT client 1 and MCPTT client 2 set up a security association (when no functional alias is present), if end-to-end encryption is used for this call.

4. The MCPTT server confirms that both MCPTT users are authorized for the private call. MCPTT server verifies whether the provided functional alias, if present, can be used and has been activated for the user. The MCPTT server checks the commencement mode setting of the called MCPTT client and also checks whether the MCPTT user at MCPTT client 1 is authorized to initiate a call in manual commencement mode.

5a. If the MCPTT private call request contains a functional alias instead of an MCPTT ID as called party and if end-to-end encryption shall be applied for this call, the MCPTT server shall resolve the functional alias to the corresponding MCPTT ID(s) for which the functional alias is active and responds with a functional alias resolution response message that contains the resolved MCPTT ID back to MCPTT client 1.

NOTE 2: If the MCPTT server detects that the functional alias used as the target of the private call request is simultaneously active for multiple MCPTT users, then the MCPTT server can proceed by selecting an appropriate MCPTT ID based on some selection criteria. The selection of an appropriate MCPTT ID is left to implementation. This selection criteria can include rejection of the call, if no suitable MCPTT ID is selected.

5b. If the MCPTT server replies with a MCPTT functional alias resolution response message, the MCPTT client 1 sends a new MCPTT private call request towards the resolved MCPTT ID.

NOTE 3: MCPTT client 1 and MCPTT client 2 set up a security association for the media, if end-to-end encryption is used for this call.

6. The MCPTT server includes information that it communicates using MCPTT service, offers the same media types or a subset of the media types contained in the initial received request and sends an MCPTT private call request for the call to MCPTT client 2, including the MCPTT ID and, if available, the functional alias of the calling MCPTT user 1. If the called MCPTT user has registered to the MCPTT service with multiple MCPTT UEs and has designated the MCPTT UE for receiving the private calls, then the incoming MCPTT private call request is delivered only to the designated MCPTT UE.

7. MCPTT server may provide a progress indication to MCPTT client 1 to indicate progress in the call setup process.

NOTE 4: Step 7 can occur at any time following step 5b, and prior to step 8b.

8a. The MCPTT user is alerted and may display the functional alias of calling MCPTT user 1. MCPTT client 2 sends an MCPTT ringing to the MCPTT server.

8b. The MCPTT server sends an MCPTT ringing to MCPTT client 1, indicating that MCPTT client 2 is being alerted.

9. MCPTT user 2 has accepted the call using manual commencement mode (i.e., has taken some action to accept via the user interface) which causes MCPTT client 2 to send an MCPTT private call response to the MCPTT server. If MCPTT user 2 has not accepted the incoming call, the MCPTT client 2 sends a call failure response to the MCPTT server without adding reason for call failure.

10. The MCPTT server sends an MCPTT private call response to MCPTT client 1 indicating that MCPTT user 2 has accepted the call, including the accepted media parameters.

11. The media plane for communication is established. Either user can transmit media individually when using floor control. For successful call establishment for private call with floor request from MCPTT client 1, the floor participant associated with MCPTT client 1 is granted the floor initially. At the same time the floor participant associated with MCPTT client 2 is informed that the floor is taken. The meaning of the floor request (give floor initially to originator [client 1], or give floor initially to target [client 2]) may be configurable. For a private call without floor control both users are allowed to transmit simultaneously.

\* \* \* End of Change \* \* \* \*